



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,177	11/05/2003	Jiwu Jing	9896-000013	7521
27572	7590	11/22/2006	EXAMINER	
HARNESS, DICKEY & PIERCE, P.L.C. P.O. BOX 828 BLOOMFIELD HILLS, MI 48303			TURCHEN, JAMES R	
			ART UNIT	PAPER NUMBER
			2112	

DATE MAILED: 11/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/702,177	JING ET AL.
	Examiner	Art Unit
	James Turchen	2112

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 05 November 2003.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-18 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 05 November 2003 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date: _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>02/26/2004</u> | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION***Priority***

Acknowledgment is made of applicant's claim for foreign priority based on an application filed in CN on September 28, 2001. It is noted, however, that applicant has not filed a certified copy of the CN application as required by 35 U.S.C. 119(b).

Drawings

Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 8-18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. It

Art Unit: 2112

is unclear how c and a are used in "sum of t first sub-secret-keys dji and a second sub-secret-key ca; wherein d, t, c, j, i and a all are positive integers". Applicant lists c and a as positive integers in the summary of the invention and in claim 8, but it is unclear how c and a are intended to be used. Applicant lists c_a throughout the detailed specification.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 3, 4, 5, 6, and 7 rejected under 35 U.S.C. 102(b) as being anticipated by Frankel et al. (US 6,035,041).

Regarding claim 1: A digital certificate issuing system with intrusion tolerance ability, comprising: at least one online task distributor (column 4 lines 25-29), k online secret share calculators (column 4 lines 48-58), m online secret share combiners (column 5 lines 32-35) and an offline secret key distributor (column 4 lines 33-37); wherein said online task distributor is connected to said k secret share calculators through a first broadcast channel, said k secret share calculators are connected to said m secret share combiners through a second broadcast channel, said offline secret key distributor is connected to said k secret share calculators and m secret share combiners during system initialization or configuration process (column 3 lines 62 through column 4 line 2 and column 4 lines 59-62); wherein k and m are positive integers.

Art Unit: 2112

Regarding claim 2: The system of claim 1, further comprising an independent output interface device connected to m secret share combiners through a third broadcast channel (column 3 lines 62 through column 4 line 2 and column 4 lines 59-62).

Regarding claim 3: The system of Claim 1, wherein an output interface device that is connected to said m secret share combiners through the first broadcast channel is set in (column 5 lines 3-14).

said online task distributor.

Regarding claim 4: The system of claim 1, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers (column 5 lines 3-14).

Regarding claim 5: The system of claim 2, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers (column 5 lines 3-14).

Regarding claim 6: The system of Claim 3, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers (column 5 lines 3-14).

Regarding claim 7: The system of claim 1, wherein the first broadcast channel and the second broadcast channel are channels connected physically or independent channels

Art Unit: 2112

not connected at all (column 3 lines 62 through column 4 line 2 and column 4 lines 59-62).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The pertinent art discloses threshold systems, methods of key hiding and exchange, and intrusion tolerant key exchange.

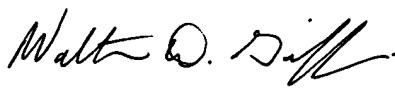
Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walt Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Art Unit: 2112

JRT



WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER